



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Hn

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/044,019	01/11/2002	Partha Bhattacharya	50325-0629	8175
29989	7590	05/26/2005	EXAMINER	
HICKMAN PALERMO TRUONG & BECKER, LLP 2055 GATEWAY PLACE SUITE 550 SAN JOSE, CA 95110			ALOMARI, FIRAS B	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 05/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/044,019	BHATTACHARYA ET AL.
	Examiner	Art Unit
	Firas Alomari	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 11 January 2004.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-28 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-28 is/are rejected.
 7) Claim(s) 1-28 is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date. _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims 1-28 are presented for examination.

Specification

1. The abstract of the disclosure is objected to because of the following informalities.

Line 4 of page 5 “diffrentmay” should be “different may”

Line 18 of page 10 “sub-emtry” should be “sub-entry”

Appropriate correction is required.

Claim Objections

1. Claims 2 and 11 are objected to because of the following informalities:

Line 6 of claim 2 recites “that that” repeated word should be deleted.

Line 10 of claim 2 recites “that that” repeated word should be deleted.

Lines 14 and 15 of claim 11 recite “and and” repeated word should be deleted.

Appropriate correction is required.

2. claim 1-28 are objected to for the following reason. The claim language must be more specific for Examiner to understand and be able to search for the invention. The claims as presented cause massive ambiguities, which make examination highly difficult. Examiner will interpret the claims to their broadest reasonable interpretation until a more clear presentation of the claims has been displayed.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. Claims 1, 2, 6, 7, 9, 10, 11, 17, 18, 22, 23, 24, 28, 23, 24, 25, 26 and 28, recite the terms "one or more" or "two or more". The limitations in the claim language do not provide a standard for ascertaining the scope of the invention and what is included and excluded by the claims. Examiner will interpret the claims to their broadest reasonable interpretation.

6. Claims 8 and 24, recite the terms "one hundred or more". The limitations in the claim language do not provide a standard for ascertaining the scope of the invention and what is included and excluded by the claims. Examiner will interpret the claims to

their broadest reasonable interpretation.

Any claims not specifically addressed are rejected by virtue of dependency.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 17, 24, 25 and 8 are rejected under 35 U.S.C. 102(e) as being anticipated by Gai et al. US (6,651,096).

Regarding claims 1, 17 and 25: A method of comparing access control lists to configure a security policy on a network, the method comprising the computer-implemented steps of:

Identifying one or more first sub-entries in a first access control list;(Col 9, Lines 49-54)

Identifying one or more second sub-entries in a second access control list;(Col 10, lines 6-13)

Programmatically determining whether a first access control list is functionally equivalent to a second access control list in order to configure the security policy on the

network by determining whether each first sub-entry is equivalent to one or more of the second sub-entries;(Col 10, lines 27-41) and

Determining that the first access control is functionally equivalent to the second access control list only when each of the first sub-entries is equivalent to one or more of the second sub-entries.(Col 10, lines 60-66, and Col, 12 line 63 through Col 13, line 6)

Regarding claims 8 and 24:Gai discloses the method as recited in Claim 1, wherein programmatically determining whether a first access control list is equivalent to a second access control list includes determining whether the first access control list having one hundred or more entries is equivalent to the second access control list having one hundred or more entries.(Col 7, lines 20- 29)

Regarding claim 26: Gai discloses a policy server communicatively coupled to one or more security devices in a network to configure a security policy on a network, the policy server comprising:

a processor; (Col 5, line 67 through Col 6, line 1)

a network interface that communicatively couples the processor to the network to receive one or more flows of packets therefrom; (Col 5, lines 61-66)

a memory; (Col 6, lines 1-7) and

one or more sequences of instructions in the memory which, when executed by the processor(Col 6, lines 13-30), cause the processor to carry out the steps of:

Identifying one or more first sub-entries in a first access control list;(Col 9, Lines 49-54)

Art Unit: 2136

Identifying one or more second sub-entries in a second access control list;(Col 10, lines 6-13)

Programmatically determining whether a first access control list is functionally equivalent to a second access control list in order to configure the security policy on the network by determining whether each first sub-entry is equivalent to one or more of the second sub-entries;(Col 10, lines 27-41) and

Determining that the first access control is functionally equivalent to the second access control list only when each of the first sub-entries is equivalent to one or more of the second sub-entries.(Col 10, lines 60-66, and Col, 12 line 63 through Col 13, line 6)

Regarding claim 27: Gai discloses the policy server of claim 26, wherein further comprising a memory to store a plurality of access control lists(Col 6, lines 15-18), including the first access control list and the second access control list(Col 7, line 60 through Col 8, line 6), and wherein the processor is configured to configure each security device on the network with at least one of the plurality of access control lists. (Col , lines Col 11, lines 47-58)

3. Claims 9-11 and 14-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Lakshman et al. US (6,289,013).

Regarding claim 9: Lakshman discloses a method of comparing access control lists to configure a security policy on a network, the method comprising:

Art Unit: 2136

identifying a dimensional range and a policy action for each entry in a first access control; (Col 6, lines 45-52)

identifying all overlapping dimensional ranges in the first access control list, each overlapping dimensional range corresponding to where the dimensional ranges of two or more entries in the first access control list overlap;(Col 6, Lines 12-18)

identifying all non-overlapping dimensional ranges in the first access control list (Col 6, Lines 53-56), each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the first access control list that do not overlap dimensional ranges of other entries in the first access control list;(Col 5, line 61 through Col 6 line 5)

identifying a policy action for each identified overlapping dimensional range of the first access control list;(Col 7, Lines 26-36)

identifying a policy action for each identified non-overlapping dimensional range of the first access control list; (Col 7, Lines 26-36) and

determining whether each identified overlapping and non-overlapping dimensional range identified from the first access control list is contained by or equal to a dimensional range of one or more entries in a second access control list in which the one or more entries of the second access control list have the policy action of that identified overlapping or non-overlapping dimensional range.(Col 7, Lines 16-26)

Regarding claim 10 and 11: Lakshman the method as recited in Claim 9, further comprising:

Art Unit: 2136

identifying a dimensional range and a policy action for each entry in the second access control; (Col 6, lines 45-52)

identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of two or more entries in the second access control list overlap; (Col 6, Lines 12-18)

identifying all non-overlapping dimensional ranges in the second access control list, (Col 6, Lines 53-56) each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list; (Col 5, line 61 through Col 6 line 5)

identifying a policy action for each identified overlapping dimensional range in the second access control list; (Col 7, Lines 26-36)

identifying a policy action for each identified non-overlapping dimensional range of the second access control list; (Col 7, Lines 26-36) and

determining whether each identified overlapping and non-overlapping dimensional range identified from the second access control list is contained by or equal to a dimensional range of one or more entries in the first access control list in which the one or more entries of the first access control list have the policy action of that identified overlapping or non-overlapping dimensional range. (Col 7, Lines 16-26)

Regarding 14: Lakshman the method as recited in Claim 9, wherein identifying a dimensional range and a policy action for each entry in the first access control list

includes identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.
(Col 5, Lines 38-48)

Regarding claim 15: Lakshman the method as recited in Claim 9, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list. (Col 6, lines 28-44)

Regarding claim 16: Lakshman discloses the method as recited in Claim 9, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a communication protocol for communication packets specified by each of the entries in the first access control list. (Col 6, lines 28-44)

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 2-7 and 18-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gai et al. US (6,651,096) in view of Lakshman et al. US (6,289,013).

Regarding claims 2, 18 and 28: Gai discloses the method according to claim 1, wherein the determining whether the first ACL is equivalent to the second ACL includes using a BBD representation but he doesn't disclose identifying a dimensional range in each policy action and determining the equivalency using the dimensional range. however Jiang disclose the method for processing an ACL where he teaches representing the table using a dimensional range(Col 4, lines 48-59), his method includes the steps of Identifying a dimensional range for each policy action specified in the access control lists (Col 6, lines 47-52 and item 402 of FIG. 4), the dimensional range of each policy action characterizing communication packets specified by one or more entries in the first access control list for that that policy action;(Col 5, lines 38-59); and determining whether the dimensional range identified for each policy action in the first access control list is equivalent to the dimensional range identified for each policy action in the second access control list. (Col 7, lines 16-25). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Gai method with teaching of Lakshman to Identifying a dimensional range for each policy action specified in the access control lists and using the dimensional range to determine if the first policy is equivalent to the second policy. One would be motivated to do so because using multidimensional representation for the ACL's will provide an easier to process

Art Unit: 2136

mathematical representation for the ACL and improve the performance of the operations being performed. (Col 3, lines 24, 36)

Regarding claims 3 and 19: Lakshman discloses the method as recited in Claim 2, wherein identifying a dimensional range for each policy action specified in the first access control list and in the second access control list includes identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list and in the second access control list. (Col 5, Lines 38-48)

Regarding claims 4 and 20: Lakshman discloses the method as recited in Claim 2, wherein identifying a dimensional range for each policy action specified in the first access control list and in the second access control list includes identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list and in the second access control list. (Col 6, lines 28-44)

Regarding claims 5 and 21: Lakshman discloses the method as recited in Claim 2, wherein identifying a dimensional range for each policy action specified in the first access control list and in the second access control list includes identifying a communication protocol for communication packets specified by each of the entries in the first access control list and in the second access control list. (Col 6, lines 28-44)

Regarding claims 6 and 22: Gai discloses the method as recited in Claim 1, wherein the first access control list and the second access control list each specify a plurality of entries, (Col 7, lines 20-28) but he doesn't disclose each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein programmatically determining whether a first access control list is equivalent to the second access control list includes: Determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of one or more entries in the second access control list that specify the policy action of the entry in the first access control list. However Lakshman disclose the method for processing an ACL where he teaches representing the table using a dimensional range (Col 4, lines 48-59), his method includes the steps of Identifying a dimensional range for each policy action specified in the access control lists (Col 6, lines 47-52 and item 402 of FIG. 4), the dimensional range of each policy action characterizing communication packets specified by one or more entries in the first access control list for that that policy action; (Col 5, lines 38-59); and determining whether the dimensional range identified for each policy action in the first access control list is equivalent to the dimensional range identified for each policy action in the second access control list. (Col 7, lines 16-25). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Gai method with teaching of Lakshman to Identifying a dimensional range for each policy action specified in the access control lists and using the

dimensional range to determine if the first policy is equivalent to the second policy. One would be motivated to do so because using multidimensional representation for the ACL's will provide an easier to process mathematical representation for the ACL and improve the performance of the operations being performed. (Col 3, lines 24, 36)

Regarding claims 7 and 23: Gai discloses the method as recited in Claim 1, wherein the first access control list and the second access control list each specify a plurality of entries, (Col 7, lines 20-28), and but he doesn't disclose each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein programmatically determining whether a first access control list is equivalent to the second access control list includes:

Determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of one or more entries in the second access control list that specify the policy action of the entry in the first access control list. However Lakshman disclose the method for processing an ACL where he teaches representing the table using a dimensional range (Col 4, lines 48-59), his method includes the steps of Identifying a dimensional range for each policy action specified in the access control lists (Col 6, lines 47-52 and item 402 of FIG. 4), the dimensional range of each policy action characterizing communication packets specified by one or more entries in the first access control list for that that policy action;(Col 5, lines 38-59); determining whether each entry in the first access control list has a

Art Unit: 2136

dimensional range that is either equivalent to or contained by the dimensional range of one or more entries in the second access control list that specify the policy action of the entry in the first access control list; (Col 7, lines 16-25) and determining whether each entry in the second access control list has a dimensional range that is either equivalent to or contained by the dimensional range of one or more entries in the first access control list that specify the same policy action.(Col 8, lines 31-43). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Gai method with teaching of Lakshman to Identifying a dimensional range for each policy action specified in the access control lists and using the dimensional range to determine if the first policy is equivalent to the second policy. One would be motivated to do so because using multidimensional representation for the ACL's will provide an easier to process mathematical representation for the ACL and improve the performance of the operations being performed. (Col 3, lines 24, 36)

3. Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lakshman et al. US (6,289,013) in view of Gai et al. US (6,651,096).

regarding claim 12: Lakshman doesn't explicitly disclose the method as recited in Claim 9, wherein identifying a policy action for each identified overlapping dimensional range of the first access control list includes using a conflict rule to determine the policy action from a first policy action of a first entry having a dimensional range within the overlapping dimensional range, and from a second policy action of a second entry

having a dimensional range within the overlapping dimensional range, wherein the second policy conflicts with the first policy. However Gai disclose a method for evaluating access control lists where he teaches the using of a conflict rule to determine the policy action when there is a conflict between two policies (Col 12, lines 42-62). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Lakshman invention with the teachings of Gai to include a conflict rule to determine the policy action when there is a conflict. One would be motivated to do so in order to enable the system to prioritize the possibly conflicting actions output by policies assigned to a given network device thus.(Col 4, lines 3-5)

Regarding claim 13: Gai discloses the method as recited in Claim 12, wherein using a conflict rule to determine the policy action selecting one of the first policy or the second policy based on the selected first or second policy being newer.(13, lines 7-24)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached on M-F from 7:30 am - 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari
Examiner
Art Unit 2136

FA


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100